Imminent-Threats of Cloud Computing Technology in Healthcare Operation

Joseph O. Esin
Professor of Computer Information Systems/Cybersecurity
Jarvis Christian College, Hawkins, Texas USA
Moses A. Agana
Senior Lecturer, Head of Department
University of Calabar, Computer Science Department
Ofem A. Ofem
Senior Lecturer, Immediate-Past Head of Department
University of Calabar, Computer Science Department
Prince Ana
Lecturer, Department Computer Science
Cross River State University of Technology, Calabar, Nigeria
Bassey E. Ele
Lecturer, Head of Department
University of Calabar, Department of Computer Science.
Paultu Tawo Bukie-Achu
Lecturer, Head of Department
University of Calabar, Department of Computer Science.
Emmanuel Oyo-Ita
Lecturer, Department Computer Science
Cross River State University of Technology, Calabar, Nigeria
Sylvester Ele
Lecturer, Department of Computer Science
University of Calabar, Department of Computer Science

Abstract

Most healthcare organizations are rapidly moving toward cloud computing technology as it is a reliable source of secured storage center and easily accessible through the Internet. Traditional hard drive storage containing organization resources, program and data are often vulnerable to untimely breakdowns, low service utilization, gross inefficiency, and inflexibility especially at a time when organizations desire stable and continued network operations. As such, cloud computing technology is a promising and attractive secured storage center for vital healthcare patient data and records. Remarkably, cloud computing technology operations are designed for multiple organizations and functions with the flexibility to accommodate healthcare facilities, private and public organizations and educational enterprises.

Overview of Cloud Computing Technology (CCT)

Most organizations are comfortable with (CCT) and currently adopting cloud computing technology as part of the security operation. Indeed, cloud computing technology is scalable, flexible, accessible, apparently self-content, challenging, though slightly inadequate and unstable in terms of security operations (Murphy, 2015 & Esin 2017). Current and future clients of cloud computing technology providers stay ahead of imminent threats to data security by initiating integrated solutions to help disrupt life-cycle cyber-attack. Private and public organizations, healthcare industry and higher education enterprises are turning to cloud computing technology as proactive solutions against cyber-attacks, loss of data and intellectual property. As Murphy (2015), Givens (2015), and Burton & Bessette (2015) maintain, any proactive counterattack approach is an added value and effective measure against a wide-range of cybersecurity-threats, cyber-crime, social engineering, ethical hacking such as script kiddies, green hackings, white hat hackers, black hat hackers and gray hat hackers. Today, cloud computing technology present a model for enabling omnipresent, convenient and on-demand network access to shared pool of configurable computing resources such as network servers, security storage, system software applications with minimal administrative and supervisory activities. The Evolving cloud computing technology is on the threshold of subsuming existing organization security network centers and defense system designed to manage organizations' information technology (IT) network security centers. Per Gray (2011) and Reese (2009), cloud computing technology is designed to restructure organization network infrastructure, computer security centers and service consolidation in order to enhance cost savings. Furthermore, cloud computing often serves as service provider empowered with ability to develop and support security facilities by limiting access to desired sections of web-based application programs only to authorized users. The goal of cloud computing technology is to function as a leading provider for outsourcing of private and public organization and higher education enterprise's security data centers. It provides physical storage space; thereby, reducing cost of upgrading of system application programs.

Framework Cloud Computing Technology

Cloud technology provides security defense to the healthcare industry where organizations' network systems are monitored and maintained by a third-party provider. Murphy (2015) noted that most of healthcare organizations are resisting adopting cloud technologies as solutions that must include compliance to cloud service provider regulations which are reliable, scalable, affordable and meet regulatory requirements. However, most healthcare organizations are slowly realizing the importance of protecting data, and information and local hard drive and alternative centers caused by understaffed and underfunded facilities. Cloud computing technology operations are not infallible and waterproof; rather, CCT constitute a dynamic protective, tenable, determined and better-secured operation and compatible than the current one-way healthcare center system (Reese, 2009 & Ngwang, 2016). Cloud computing technology exits to relieve citizens from extensive cost of healthcare services, by moving substantial portion of data, applications programs and resources to cloud computing technology for security center. As a result of cost pressures, budget constraint, and the inability to secure data, patient records have created an ample corridor for healthcare organizations to re-evaluate existing security centers to relieve

IT members from a labor-intensive, auditing and updating software programs to smaller agile teams of skilled high-tech professionals.

Cloud computing technology is reliable, secured storage center that can protect, store and retrieve data faster on-site lead IT employees. It is quite certain that if massive data and information are left unattended on only one locale, without intelligent analytics, knowledgeable security professionals, the organization will be deemed worthless to vulnerable clients and healthcare population (Smith ,2008; Smith, 2015; and Gray, 2011). Cybercriminals are continually gathering intelligence on cloud computing technology security solutions to gain access to information and to reduce-visible communicative patterns to conceal malicious actions.

Providers often take control of sensitive data and applications in order to hold cybercriminals at bay and to be able to respond to cyber-threats prior to data leaving the data security facility. The breach of patients' data and records is the greatest threat to any healthcare organization's security and constitutes prime vulnerability access points to protective facility. Per Reese (2009) and Murphy (2015), 75% of cybercriminal attacks takes few minutes for data ex-filtration, and approximately 50% of breaches often stick around for months. These breaches caused within a few minutes often undetermined human activities and financial resources to remedy impending security operations. This paucity in security therefore justifies and intensifies the use of cloud computing technology to monitor incoming and outgoing email activities and internet access to protect and prevent cybercriminals from hacking into healthcare organizations' security data center. Cloud computing technology is designed to assist healthcare facilities to combat challenges relating to the chasm created between data stored in the local hard drive and cloud computing technologies, and a host of vital data in a foreign and far-off data storage. As Reese (2009) and Gray (2011) noted, real-world setbacks on outlying cloud computing technology operation centers often occurs if:

- Cloud providers declare bankruptcy, obliging storage data centers to cease to operate and control the system and thereby possibly handing these operations over to competitors;
- Competitors who do not recognize current clients' contractual agreements sue cloud providers to obtain a blanket subpoena granting unlimited access to cloud clients' servers; and
- Cloud fails to provide proper security in maintaining physical infrastructure and adequate access resulting in compromising clients' data.

The nucleus of healthcare organizations is the well-being of patients and the protection of medical records and data, regardless of data location, encryption of data, encryption of backup data located on on-site and off-site location. It also includes procedures to safeguard the organization's data, information and medical records. As Castaldo (2015) noted, cloud computing technology is intended to alleviation IT Directors from hardware and software maintenance, upgrading, scheduled backups and configuration. The IT team must be prepared to create structures where historical data can be retrieved and recovered if cloud computing technology operations close and vanish from the face of the planet. Several storage alternatives have been introduced as safety measures. For instance, the Bring-your-own-device (BYOD) in healthcare organization is at epidemic magnitudes and most patients prefer using Apple MacBook, iPads, Android tablets, and smartphones to protect vital data and information. Most healthcare organizations, patients and physicians who know risks have declined this method and resorted to using standard Windows laptops for official health assessment, diagnosis, treatment and prescriptions sent to patients' pharmacy. Mobile applications used by healthcare teams contain the organization's and patients' vital records. However, the continued usage of configured personal devices often expose most organization's network operations to security risks. 98% of application programs written for Android platform contain gaping security vulnerabilities and unsafe practices. Unfortunately, most IT professionals often do not have skilled personnel and resources to mitigate the network operation (Reese, 2009). Since BYOD and mobile threats change constantly due to the proliferation of new mobile applications, healthcare organizations must incorporate adaptive technologies to manage identities, control and monitor data access. Cyber-criminals repeatedly use mobile devices to launch attacks and to neutralize predetermined sophisticated threats. To contain or circumvent these threats, Fitzgerald & Schneider (2015) suggested that IT professional teams must establish network visibility operation, intelligence and efficient response, collaborative alliance and information sharing partnership amongst healthcare organizations and patients' population. Privacy data and information must always be protected. Confidentiality of organization data and information varies depending on the organizations, entity and locations covered. However, the mystery behind privacy of data is open for deliberation and conformation of what constitutes privacy of patient data.

Benefits of Cloud Computing Technology

Cloud computing technology are often designed to be reliable, allowing small and medium size organizations to strive alongside with large corporation and to enable all sizes of organizations to operate using large external hard drive to access community information anytime, and anywhere. Per Gray (2011), Esin (2017), and Murphy (2015), most healthcare network folders and file servers often have redundancies designed to endure hardware and software installations and configurations processes. Associated advantages of cloud computing technology include retaining and managing network files servers and protecting them against hardware malfunction, power outages, system failure, flood, hurricane, extreme cold and heat, ongoing upgraded, hardware and software installations, configurations, troubleshooting and regular network maintenance. Managing and maintaining traditional network files servers is frequently an overwhelming, task-oriented process designed to free most organizations from underlying hardware, software installation and software application upgrades, auditing and management. The evolution of cloud computing technology services is enabling and facilitating healthcare organizations to pay closer attention to patients' records and data security centers.

Most healthcare organizations are rapidly moving toward cloud computing technology as it is a reliable source of secured storage accessible through the Internet. Traditional hard drive storage often results in untimely breakdown, low service utilization, gross inefficiency, and inflexibility in responding to organization's desire for stable and continued network operations. Cloud computing technology is a promising and attractive storage environment for healthcare and organizations in need of alternative and reliable storage system for privacy and security of patients' data and information. Remarkably, cloud computing technology operation is designed for multiple organizations that share the same need for information storage, privacy of information and an extensive clientele such as consumers and financial institutions, educational enterprises and government agencies (Gray, 2011; Esin, 2017; Murphy, 2015).

Cloud computer technology has tremendous advantages which include increased efficiency in handling services, data and information which are rapidly deployed for use in a matter of minutes versus weeks and months of delay. As Gray (2011), Dubai (2008) and Kinyenje (2015) noted, five traditional benefits outside efficiency in the use of cloud computing technology include business agility, new businesses, less operations issues, better use of resources and less capital expense. B**usiness agility incorporates items** such as getting the needed computer resources on a scheduled time, having the ability to deliver results faster through inexpensive operation and quality service that might challenge competitors. New **business models enhance the** ability to create a better opportunity for innovation initiatives often generating new value propositions and resulting in new revenue streams. **Less operational issues act involves** establishing traditional standardized service operations to reduce defects, increase business continuity, reduce time spent on unproductive issues and focusing on the mission-driven operation of the organization. Cloud computing technologies tend to allow the deployment of the matching topology of services repetitively, with the same result every time and enabling organizations to deploy pre-build file server images, application services and entire application landscapes. Such initiatives result in b**etter use of resources involving** business agility model that often leads to efficient projects and less operational service, freeing customers and IT personnel to spend more time gainfully on productive activities with greater potential value to the organization. However, benefits differ from one organization to the other, as organizations acquire bigger assets and managerial expertise and progress and l**ess capital expense**. Most often, an organization's value tends to shift from a capital expense (Cap Ex) model to an operational expense (Op Ex) model. The overall sentiment is that specifically for short and midterm projects, the Operational Expense model is more attractive because there are no long-term financial commitments. The Operational Expense model often produces zero upfront investment, allowing organizations to start projects faster; ultimately, they end up without losing any investments in the cloud services. Cloud computing technology services are accessed through a web browser like Microsoft Internet Explorer, Microsoft Edge, Mozilla Firefox, or Google Chrome. Per Reese's (2009) assessment, cloud computing technologies constituent relationship management (CRM) database system is an alternative to hosting patient data and records in organization's security storage center.

Per Esin (2018) and Gray (2011), four major layers of cloud computing technology component includes Cloud Clients, SaaS-applications, PaaS-platform and IaaS-infrastructure. Cloud computing layers vary slightly from one layer to the next and generally classify infrastructure as a service, platform as a service, and software as a service.

Layer One

Cloud Client's Web Browser, Mobile Applications,

Thin Client and Terminal Emulator.

Layer Two

Software as a Service (SaaS) Application
CRM, Email, Virtual Desktop, Communication and Games.

Layer Three

Platform as a Service (PaaS) Platform
Execution Runtime, Database, Web Server and Development Tools.

Layer Four

Infrastructure as a Service (IaaS) Infrastructure
Virtual Machines, Servers, Storage, Load, Balancers and Network. Cloud-based Voice over Internet Protocol **(VoIP) telephone service**

Software as a Service (SaaS)

SaaS layer is an Internet-based software service available for purchase and rent on a per-user, per-month basis. It is the most common type of cloud service for individuals and small businesses and offices. Indeed, SaaS applications are highly customer-oriented and do not require skill and technical expertise for day-to-day operation and maintenance.

Platform as a Service (PaaS)

PaaS layer often provides users with framework and set of functions that can be customized and used to develop applications such as Google App Engine.

Infrastructure as a Service (IaaS)

IaaS is the foundation layer of cloud computing technology set up like storage, backup, and security to include database, storage, virtual private server, and support services that are available on demand by the hour.

Potential Advantages of Cloud Computing

Per Lewis and Baker (2014) and Gray (2011), Cloud Computing Technology holds a lot of exciting potential for all sizes of private and public organizations ready and willing to realize cost savings through maintaining the organization's server to enable new levels of sharing and collaboration. Cloud computing technology was created to reinforce and promote greater network system transparency and increased need for effective organization operations. It was equally created to break down the barriers in communication and sharing useful information and to enhance effective and durable organizations.

Cloud Computing Technology Professional Engagement

1. Agana has been retained as the current Head of Department, Computer Science Department at the University of Calabar. He notices that Ofem, immediate past head of department of computer science used Internet-delivered inventory, storage and backup solutions during his two years in the office. What type of cloud computing technologies will be appropriate for Agana's operation? **(Circle only one correct answer)**
   a. **Private cloud technology**
   b. **Public cloud technology**
   c. **Retail cloud technology**
2. Bukie-Achu is scheduled to resume appointment as a department software developer and has opted to build and test the institution Web application through cloud computing technologies apparatus. Identify the type of cloud computing technology that is appropriate for the operation **(Circle only one correct answer).**
   a. **PaaS**
   b. **SaaS**
   c. **IaaS**
   d. **XaaS**
3. Ana, Ofem's deputy is considering using security storage system to protect and manage patient medical records data and information located in application programming interface (API) unit. Identify the type of cloud computer technology service that is appropriate for the operations **(Circle only one correct answer).**
   a. **IaaS**
   b. **PaaS**
   c. **CaaS**
   d. **SaaS**
4. Oyo-Ita is increasingly uncomfortable with non-inclusive cloud computing technologies operation and demands inclusion of the department of computer science, department of statistics and department of mathematics as active members of this vital service. Identify the model of cloud computing technologies that will satisfy Oyo-Ita's all-inclusive operation. Curiosity **(Circle only one correct answer).**
   a. **Public cloud technology**
   b. **Network cloud technology**
   c. **Community cloud technology**
   d. **Private cloud technology**
5. Ofem's immediate-past head of department of computer science at the University of Calabar used these three model cloud computing technologies service: model 1 often

requires the institution to deploy existing operating systems, applications, software program onto the provided infrastructure, model 2 represents a software environment that runs on top of the infrastructure and model 3 frequently provides universal access to authorized users to a single copy of an application. Identify a compatible operating system that best satisfies Ofem's modus operandi **(Circle only three correct answers).**

a. **Platform a Service, Infrastructure as a Service and Software as a Service**
b. **Planform as a Service, Platform as a Software and Application as a Service**
c. **Infrastructure as a Service, Application as a Service and Software as a Service**
d. **Infrastructure as a Service, Platform as a Service and Software as a Service**

6. Ele I and Ele II notify the head of department of computer science at the University of Calabar that Cloud-based computer technology is designed to provide account provision, administration, management, authentication, authorization, reporting and monitoring capabilities. In which component of cloud computing technologies service will the service be located? **(Circle only one correct answer).**

a. **PaaS**
b. **DaaS**
c. **IaaS**
d. **SaaS**

7. Per Esin (2018) most private and public organizations' and higher education enterprises' ultimate, supreme and paramount apprehension about cloud computing technologies is on. **(Circle only one correct answer).**

a. **Availability**
b. **Security**
c. **Elasticity**
d. **Redundancy**

Scholarly Engagement Solutions

1. C

2. A

3. A

4. C

5. C

6. C

7. B

References

Burton, Sharon L. & Bessette, Dustin. (2015). War Against Identity Cyber Assault in a Social World. *The United States Cyber Security Magazine*. 2 (1) 16-17.

Castaldo, Chris . (2015). Why the Internet of Things, doesn't have to be a Security Nightmare. *The United States Cyber Security Magazin*e 3 (7) 16-17.

Dubai, UAE. (2008). Information Technology's role in providing high quality healthcare. Booz

& Company. White Paper (2015) *Combating Cybercrime in the Healthcare Industry*: Cisco and affiliates.

Esin, Joseph O. (2017). "Escalating Outcome of Cyber-Attacks on Healthcare Organizations". Washington Center for Cybersecurity Research and Development. https://www.washingtoncybercenter.com/publications-projectsFitzgerald,

Fitzgerald, Alvita & Schneider, Jessica (2015). "Keep it Secret, Keep it Safe: Nine Steps to Maintaining Data Security." The United States Cyber Security Magazine, Volume 3, Number 7(74-75).

Gray, Mike (2011). "Cloud Computing: Demystifying IaaS, PaaS, and SaaS," ZDNET,http://www.zdnet.com/news/cloud-computing-demystifying-iaas-paas-and- saas/477238.

Kinyenje, Christine. (2015). *Strategizing for Data Breach Risk Management. United States Cybersecurity, Magazine* 3 (8), 74-76.

Lewis, James A. & Baker, Stewart. (2014). Estimating the Cost of fighting cybercrime. Accessed 2/10/2014 from Https://csis.org/event/estimating-costcyber-crime-andcyber-espionage.

Murphy, Sean P. (2015). *Healthcare Information Security and Privacy.* San Francisco, CA: McGraw Hill.

Ngwang, Emmanuel N. (2016). Individual freedom, cyber security and the nuclear proliferation in a borderless land: Innovations and trade-offs in scientific progress. *The Journal of Educational Research and Technology (JERT)* 5 (5) 17-38.

Reese, George. (2009). Cloud Application Architecture: Building Applications and Infrastructure in the Cloud. *O'Reilly Media.* Graven Stein Highway North, Sebastopol: CA.

Smith, Christen Marie. (2015). Building the Cyber force of the Future. *United States Cybersecurity 3 (9) 43-55.*

Smith, John C. (2008). *History of the High Technology Crime Investigation Association* (HTCIA): Santa Clara (Silicon Valley) CA.